PAN-OS® 6.1.4 Release Notes

PAN-OS 6.1 Release Information

This release note provides important information about Palo Alto Networks PAN-OS 6.1 software, including an overview of new features introduced in this release and a list of known issues. For instructions on how to upgrade the firewall to PAN-OS 6.1 and configure the new features, refer to the New Features guide.

For the most up-to-date information, refer to the online version of the PAN-OS 6.1 Release Note on the Technical Documentation portal.

Features Introduced in PAN-OS 6.1

The following topics describe the new features introduced in the PAN-OS 6.1.0 release. Content Release version 454 is required to use some of the new features in this release. For details on how to use the new features, refer to the New Features Guide.

Management Features

The following Management features are introduced in PAN-OS 6.1.0. For more details about these features and for instructions on configuring them, refer to Management Features in the New Features Guide.

New Management Feature	Description
Security Policy Rulebase Enhancements	The security policy rulebase enhancements enable more streamlined control over intrazone (within a zone) and interzone (between zones) traffic. With these enhancements, you can now create rules that enable visibility and control over intrazone or interzone traffic for multiple zone pairs in a single rule rather than having to create separate rules for each pair. To enable this flexibility, a new Rule Type classification indicates whether the rule matches intrazone traffic, interzone traffic, or both intrazone and interzone (called universal) traffic. The default Rule Type is universal. When you upgrade to PAN-OS 6.1, all existing rules in your security rulebase will be converted to universal rules. In addition, the implicit default rules the firewall uses for handling intrazone and interzone traffic that doesn't match any other rules have now been exposed, allowing you to override select settings—including logging, action, and threat inspection settings—on these rules.
App Scope Enhancements	App Scope has been updated to allow for improved security and a lighter footprint. This change supports enhancements that enable you to: • Export maps, charts and images (.png or .pdf); export requires a browser that supports HTML 5 • Zoom-in and out of charts • Toggle legend entries in a chart to select the data that is displayed on the screen
Authenticated NTP	You can now configure the firewall to authenticate time updates from the NTP server used to synchronize the firewall clock. You can enable Authenticated NTP to use symmetric key exchange (shared secrets) or autokey (public key cryptography) authentication. Use Authenticated NTP to prevent tampering with the firewall clock and resulting disruptions to logging and schedule-based policies and services.
Multiple M-100 Interfaces	The Panorama™ M-100 appliance now supports the use of separate interfaces for management, device log collection, and collector group communication. Configure the eth0 (MGT), eth1, and eth2 interfaces interchangeably for one, two or all three functions. By default, the MGT interface performs all three functions but configuring separate interfaces is a best practice to improve security, control traffic prioritization, performance, and resilience.
Related Log Detail View Enhancements	To make it easier to correlate log information from a session, you can now click through the related logs in the Detailed Log View without closing the window and switching views. You can switch between the URL Filtering, Threat, Traffic, and Data Filtering logs associated with a session and the Detailed Log View window will dynamically update to display pertinent information for the selected log.
Log Forwarding Optimization	Log Forwarding has been enhanced to be more efficient and to use less CPU on all platforms.

New Management Feature	Description
Configurable Key Size for SSL Forward Proxy Server Certificates	The firewall now supports both 2048-bit RSA keys (with SHA-256 hashing) and 1024-bit RSA keys (with SHA-1 hashing) for generating the certificates it uses to establish the SSL Forward Proxy session between itself and the client. This is an extension of the 2048-bit key support that was already available with SSL decryption. In previous releases, 2048-bit keys were supported in SSL Inbound Inspection sessions as well as in SSL Forward Proxy sessions between the firewall and the destination server. As part of the extended support for 2048-bit keys, the firewall will now by default dynamically choose the key size to use to establish SSL Forward Proxy sessions with clients, based on the key size used by the destination server. You can optionally configure a static key size for SSL Forward Proxy sessions between the firewall and clients regardless of the key size used by the destination server.
Default profile group and log forwarding settings	You can now allow new security policies and new security zones to include your organization's preferred settings for security profile groups or log forwarding by default. Create a *default* security profile group or *default* log forwarding profile; the *default* profile group will be attached to new security policies automatically and the *default* log forwarding profile will be selected for new security policies and new security zones automatically. With a *default* security profile group and a *default* log forwarding profile configured, you can quickly create new security policies and security zones without manually selecting your preferred settings for log forwarding or a profile group each time. This also allows you to enforce consistency for other administrators creating new policy rules or zones, by including your organization's preferred profile group and log forwarding options in new policies or zones automatically.

WildFire Features

The following WildFire™ features are introduced in PAN-OS 6.1.0. For more details about these features and for instructions on configuring them, refer to WildFire Features in the New Features Guide:

New WildFire Feature	Description
Signature/URL Generation on the WildFire Appliance	The WF-500 appliance can now generate signatures locally, eliminating the need to send any data to the public cloud in order to block malicious content. The WF-500 WildFire appliance can now analyze files forwarded to it from Palo Alto Networks firewalls or from the WildFire API and generate the following types of signatures that block both the malicious files as well as associated command and control traffic: • Antivirus signatures detect and block malicious files. These signatures are added to WildFire and Antivirus content updates. • DNS signatures detect and block callback domains for command and control traffic associated with malware. These signatures are added to WildFire and Antivirus updates. • URL Categorization classifies callback domains as malware and updates the URL category in PAN-DB. Firewalls must be running PAN-OS 6.1 or later to enable local signature generation for forwarded files. In addition, you must configure the firewalls to receive content updates from the WF-500 WildFire appliance, which can occur as frequently as every five minutes. You can optionally send the malware sample file analysis data (or just the XML report if you don't want to send the sample) to the WildFire public cloud to enable signature generation for distribution through the Palo Alto Networks update server.
Content Updates on the WF-500 WildFire Appliance	To support the ability to generate signatures on the local WF-500 WildFire appliance, daily content updates are now available for the appliance. These content updates equip the appliance with the most up-to-date threat information for accurate malware detection and improve the appliance's ability to differentiate the malicious from the benign.
Email Header Information in WildFire Logs	The firewall now captures email header information—email sender, recipient and subject—and sends it along with the corresponding email attachments and email links that it forwards to WildFire. If WildFire determines that the email attachment or link is malicious, it includes the email header information in the WildFire Submissions log that it returns to the firewall. This information can help you quickly track down and remediate threats that are detected in emails received by your users. Note that neither the firewall nor WildFire receive, store, or view the actual email contents.
Flash and Office Open XML File Type Support	Firewalls can now forward Flash content embedded in web pages to WildFire for analysis. In addition, WildFire now creates antivirus signatures for Flash applets and Office Open XML (OOXML) 2007+ documents that it determines to be malicious and delivers the signatures through antivirus updates, enabling you to alert or block malicious content in these types of files. To support this capability, the firewall must have a WildFire subscription and be running Content Release version 454 or later.

New WildFire Feature	Description
WildFire Email Link Analysis	The firewall can now extract HTTP/HTTPS links contained in SMTP and POP3 email messages and forward the links to the WildFire public cloud for analysis (this feature is not supported on the WF-500 WildFire appliance). Enable this functionality by configuring the firewall to forward the email-link file type. Note that the firewall only extracts links and associated session information (sender, recipient, and subject) from the email messages that traverse the firewall; it does not receive, store, forward, or view the email message. After receiving an email link from a firewall, WildFire visits the links to determine if the corresponding web page hosts any exploits. If it detects malicious behavior on the page, it returns a malicious verdict and: • Generates a detailed analysis report and logs it to the WildFire Submissions log on the firewall that forwarded the links. This log now includes the email header information-email sender, recipient and subject-so that you can identify the message and delete it from the mail server and/or track down the recipient and mitigate the threat if the email has already been delivered and/or opened. • Adds the URL to PAN-DB and categorizes it as malware. Note that if the link corresponds to a file download, WildFire does not analyze the file. However, the firewall will forward the corresponding file to WildFire for analysis if the end user clicks the link to download it as long as the corresponding file type is enabled for forwarding. Note also that WildFire does not send a log to the firewall if it determines a link to be benign even if you have enabled logging of benign files because of the large number of logs this would generate.
WildFire Analysis Report Enhancements	The WildFire detailed report provides new forensic details to help you quickly identify threat severity and signature coverage status: • The report now provides details about each behavior that the sample file exhibits and the corresponding Severity of each behavior. A visual gauge provides an at-a-glance indicator of severity level; one bar indicates low severity and each additional bar indicates a higher severity level. • A new Coverage Status section dynamically updates when the report is rendered on the firewall. This section displays up-to-date information about what signature and URL filtering coverage that Palo Alto Networks currently provides to protect against the threat.
Windows 7 64-bit Support	WildFire now supports the Microsoft Windows 7 64-bit sandbox environment on both the WildFire public cloud and the WF-500 WildFire appliance. Support for this environment on the WF-500 appliance requires that you upgrade the appliance OS to 6.1 and install the Windows 7 64-bit image.
WildFire XML API Support on the WildFire Appliance	The WF-500 appliance now supports the WildFire XML API. To use WildFire XML API with the appliance, you must generate the API key on the appliance. The WF-500 appliance supports up to 100 API keys.

URL Filtering Features

The following URL Filtering features are introduced in PAN-OS 6.1.0. For more details about these features and for instructions on configuring them, refer to URL Filtering Features in the New Features Guide:

New URL Filtering Feature	Description
Logging of HTTP Header Fields	To facilitate troubleshooting and forensic analysis, you can now enable logging of one or more of the following HTTP header fields in the URL Filtering profile: User-Agent, Referer, and X-Forwarded-For. The HTTP header information for each matching session will be included in the URL Filtering logs, and will also be displayed in a new widget in the Detailed Log View for URL Filtering, Threat, and WildFire logs. The HTTP header fields in URL filtering logs are also available for custom log forwarding to a syslog server and for inclusion in custom reports on the firewall and on Panorama™.
Manual Upload of BrightCloud Database	In deployments where Panorama or a firewall has no direct Internet access, you can now manually upload and install the BrightCloud database.
Full-path Categorization of URLs in PAN-DB	PAN-DB can now categorize content down to the page level instead of just at the directory level. Because the pages within a domain can belong to multiple categories, this capability provides increased accuracy in filtering content and prevents potential over-blocking of web content. If, for example, you block malware and allow access to business/ news content for users on your network, they can access http://www.acme.com/c/news.html because it is categorized as news/business, but be denied access to http://www.acme.com/c/malware.exe because PAN-DB categorizes the full-path for this web page as malware. To test the category for a full path of a valid URL, use http://urlfiltering.paloaltonetworks.com/testASite.aspx.

Virtualization Features

The following Virtualization features are introduced in PAN-OS 6.1.0. For more details about these features and for instructions on configuring them, refer to Virtualization Features in the New Features Guide:

New Virtualization Feature	Description
Support for VM-Series on Amazon Web Services (AWS)	If you are moving or have moved your servers/applications from self-managed datacenters to a Virtual Private Cloud (VPC) within the Amazon Web Services (AWS) cloud, you can now deploy the VM-Series firewall as a secure gateway to your VPC. The VM-Series firewall is available as a public Amazon Machine Image (AMI) and can be deployed on an Elastic Compute Cloud (EC2) instance. Consistent with the Amazon AWS networking requirements, VM-Series firewalls deployed in the Amazon AWS support only Layer 3 interfaces. In addition, the VM Information Sources feature on PAN-OS has been extended to monitor changes in the AWS VPC. Using the VM Information Sources feature, the firewall can connect to an Amazon VPC and collect EC2 instance IP addresses and associated metadata as tags to gain context awareness, which then allows for consistent security policy enforcement despite changes in the EC2 instance inventory.
Support for VM-Series on Kernel-based Virtual Machine (KVM)	The VM-Series firewall can be installed on 64-bit versions of Linux distributions running KVM hypervisor deployed on x86 hardware with Intel or AMD chipsets with virtualization extensions enabled. The supported Linux distributions are CentOS, Red Hat Enterprise Linux (RHEL), and Ubuntu. VM-Series firewalls deployed on KVM support e1000, virtio, PCI passthrough, and Single Root I/O Virtualization (SR-IOV) network drivers.

GlobalProtect Features

The topics in this section are the new GlobalProtect™ features introduced in PAN-OS 6.1.0. For more details about these GlobalProtect features and for instructions on configuring them, refer to GlobalProtect Features in the New Features Guide.

For information on related features introduced in the GlobalProtect Mobile Security Manager 6.1.0 release, including how to set up an enterprise app store for your users and how to isolate business traffic and data on mobile devices, refer to the GlobalProtect Mobile Security Manager 6.1 New Features Guide.

New GlobalProtect Feature	Description
Extended SSO Support for GlobalProtect Agents	With Single Sign-On (SSO), the GlobalProtect agent wraps the user's Windows login credentials to automatically authenticate and connect to the GlobalProtect portal and gateway. SSO has been enhanced in this release so that when a third-party credential provider is being used to wrap the user's Windows login credentials, the GlobalProtect agent wraps the third-party credentials to allow for successful authentication for the Windows user. This extended SSO functionality is supported on Windows 7 and Windows Vista clients.
Per App VPN for GlobalProtect iOS App	The GlobalProtect iOS app now supports Per App VPN. With Per App VPN enabled, the GlobalProtect iOS app will route all traffic from managed business apps through your corporate VPN, while personal apps that are not managed can connect directly to the Internet. An MDM service, such as the GlobalProtect Mobile Security Manager, is required to enable the GlobalProtect iOS app's per App VPN capability.
Disconnect on Idle	The options to time out GlobalProtect clients have been extended to include settings you can use to log out idle users. You can set the number of minutes after which users will be disconnected from GlobalProtect if there is no traffic going through the VPN.
Disable Browser Access to the Portal Login Page	Prevent public access to the GlobalProtect portal login page and unauthorized attempts to authenticate to the GlobalProtect portal from a web browser by disabling the portal login page. With the portal login page disabled, you can use a software distribution tool, such as Microsoft's System Center Configuration Manager (SCCM), to allow your users to download and install the GlobalProtect agent. GlobalProtect agents and apps will continue to successfully authenticate and connect to the portal to receive configuration updates.

High Availability (HA) Features

The following high availability (HA) feature is introduced in PAN-OS 6.1.0:

New High Availability Feature	Description
HA Session Sync During Upgrade from One Feature Release to the Next	Session syncing will now remain operable when upgrading HA peers from one PAN-OS feature release version to the next feature release version (for example, when upgrading the firewalls from PAN-OS 6.0.x to PAN-OS 6.1.x). Although session syncing has always been operable when upgrading from one maintenance release to another in the same feature release version (for example, during upgrade from PAN-OS 6.0.1 to PAN-OS 6.0.3), in prior releases it was inoperable when upgrading from one PAN-OS feature release to the next. This meant that if there was a failover during the period of time when the individual firewalls in the HA pair were running different feature release versions (for example, if one firewall was running 5.0.13 and the other one was running 6.0.3) sessions could have been impacted.

Networking Features

The following Networking features are introduced in PAN-OS 6.1.0. For more details about these features and for instructions on configuring them, refer to Networking Features in the New Features Guide.

New Networking Feature	Description
NAT Enhancement for Session Load Balancing	On PA-5000 Series platforms, Static Source NAT, Dynamic IP NAT, and Destination NAT session processing has been enhanced to allow the firewall to use multiple CPUs to process NAT sessions, rather than anchoring the sessions to a CPU based on destination IP hash. This enhancement greatly improves throughput in these NAT scenarios, particularly in topologies that include a load balancer or other device that limits the number of destination IP addresses. This enhancement will occur automatically upon upgrade of the PA-5000 Series device. Note that Dynamic IP and Port NAT (DIPP) or Dynamic IP NAT sessions that fall back to DIPP will continue to be anchored to a specific CPU, based on the destination IP address (the target translated address).
NAT Capacity Enhancements	The maximum number of NAT rules (static, Dynamic IP, and Dynamic IP/Port) allowed for each platform has been increased and NAT statistics now include usage and memory information to provide efficient management of NAT rules. The Dynamic IP/Port oversubscription ratio can now be tuned to allow greater control in environments requiring more Dynamic IP and Dynamic IP/Port rules. These NAT capacity enhancements are supported on PA-3000 Series, PA-4000 Series, PA-5000 Series, and PA-7050 platforms.
LACP	You can now use the Link Aggregation Control Protocol (LACP) to dynamically detect the interfaces between interconnected devices (peers) and combine those interfaces into an aggregate group. Enabling LACP provides redundancy within an aggregate group: the protocol automatically detects interface failures and fails over to standby interfaces. LACP is supported on Layer 2, Layer 3, and HA3 interfaces only and is supported on PA-500, PA-3000 Series, PA-4000 Series, PA-5000 Series and PA-7050 platforms.

New Networking Feature	Description
Remove TCP Timestamp	A new **Remove TCP Timestamp** option has been added to the Zone Protection profile to enable you to strip the TCP timestamp from the TCP header. This option is available in the web interface and in the CLI.
TCP Session Closing Timers	Two new timers have been added (TCP Time Wait and TCP Unverified RST) and the tcp-wait timer has been renamed the TCP Half Closed timer, as detailed below: • The TCP session termination procedure now has a TCP Half Closed timer, which is triggered by the first FIN the firewall sees for a session, and a second timer (TCP Time Wait), which is triggered by the second FIN or a RST. You can set these timers globally or per application. In prior releases, only one TCP wait timer existed, triggered by the first FIN. If that setting was too short, the half-closed sessions could be closed prematurely. Conversely, a setting that was too long could make the session table grow too much and possibly use up all of the sessions. By having two timers, a relatively long TCP Half Closed timer allows the opposite side time to respond, and a short TCP Time Wait timer quickly ages fully closed sessions and controls the size of the session table. • A TCP Unverified RST timer has been added at the global level. If the firewall receives a RST that cannot be verified (because it has an unexpected sequence number within the TCP window or it is from an asymmetric path), the TCP Unverified RST timer controls the aging out of the session. This timer provides an additional security measure.
Session End Reason Logging	When troubleshooting connectivity and application availability issues, knowing what caused a session to terminate can be useful. PAN-OS now provides a new session end reason field in traffic logs. Session end reasons can also be included in reports that are generated based on traffic logs and SNMP traps and email alerts that are triggered by traffic logs contain session end reasons, as well.

Changes to Default Behavior

The following points describes changes to default behavior in PAN-OS 6.1.0:

- The default key size for SSL/TLS Forward Proxy certificates has changed from 1024-bit RSA to **Defined by destination host**. The new default setting allows for PAN-OS to generate certificates based on the key that the destination server uses.
- A new **Rule Type** classification indicates whether a security rule matches intrazone traffic, interzone traffic, or both (called *universal*). In releases prior to PAN-OS 6.1.0, the rule type classification did not exist and all rules were considered universal. Existing rules in the rulebase are converted to universal rules when you upgrade to PAN-OS 6.1.0; you can then choose to change the **Rule Type** to **intrazone**, **interzone**, or leave it classified as **universal**.
- The GlobalProtect agent now collects the domain that is defined for the `ComputerNameDnsDomain` parameter from Windows clients. This is the DNS domain assigned to the local computer or the cluster associated with the local computer. The value for the parameter `ComputerNameDnsDomain` is used to populate the **Domain** displayed in the HIP Match logs for Windows clients.

Associated Software Versions

The following minimum software versions are supported with PAN-OS 6.1:

Palo Alto Networks Software	Minimum Supported Version with PAN-OS 6.1.0
Panorama™	6.1.0
User-ID™ Agent	6.0.0
Terminal Server Agent	5.0.0
NetConnect	Not supported in 6.1.0
GlobalProtect™ Agent	1.2.0
GlobalProtect Mobile Security Manager	6.0.0
Content Release Version	454

Known Issues

The following list describes known issues in the PAN-OS 6.1.0 release:

For recent updates to known issues for a given PAN-OS release, refer to https://live.paloaltonetworks.com/docs/DOC-1982.

Issue Identifier	Issue Description
74180	On PA-7050 firewalls in a high availability (HA) configuration, a TCP connection cannot be established when a virtual wire subinterface with VLAN tags and IP classifiers is configured.
72922	In a high availability (HA) active/active configuration with an IPSec tunnel configured to terminate on a floating IP address, if a session is owned by the device that does not own the floating IP address, traffic might be dropped.
72715 *This issue is now resolved. See the list of* PAN-OS 6.1.4 Addressed Issues.	An M-100 appliance in Panorama™ mode running PAN-OS 6.1.2 or PAN-OS 6.1.3 might be unable to receive logs forwarded by a managed firewall. Workaround: check that all managed firewalls are assigned to a Log Collector (**Panorama > Collector Groups > Device Log Forwarding**). Assign a Log Collector to any managed firewalls that do not have a log forwarding preference configured.
71609 *This issue is now resolved. See the list of* PAN-OS 6.1.4 Addressed Issues.	Special characters are not supported in the local portion of an email address (the text in front of @) for email addresses specified in email server profiles (**Device > Server Profiles > Email**). If you downgrade to a release earlier than 6.1.4, you should expect the following commit errors if there are special characters in the local portion of any email address in your email server profiles in PAN-OS 6.1.4 and later releases: • Pushing email addresses with special characters from PAN-OS 6.1.4 or higher releases to devices running PAN-OS 6.1.3 or earlier releases will fail. • Subsequent auto-commit events after the initial auto-commit initiated during the downgrade process to a PAN-OS 6.1.3 or earlier release will fail if email addresses in email server profiles contain special characters.
70222	If the password for the administrator's account on the NSX Manager contains special characters, such as "$", Panorama cannot communicate with the NSX Manager. The inability to communicate prevents context-based information, such as Dynamic Address Groups, from being available to Panorama. Workaround: remove special characters from the password on the NSX Manager.
69725	A log collector running a PAN-OS 6.0.X release does not correctly receive NTP server configuration settings when they are pushed from Panorama running PAN-OS 6.1.0. When both the log collector and Panorama are running PAN-OS 6.1.0, NTP server configuration settings can be successfully pushed from Panorama to the log collector.
69598	Auto-commits can fail following an upgrade to PAN-OS 6.1.0 if Aggregate Ethernet (AE) interfaces have been previously configured without defining an interface type (this can only be done using the CLI; the web interface requires for the interface type to be defined). Before upgrading to PAN-OS 6.1.0, ensure that all AE interfaces are configured as a certain type of interface: HA, Layer 2, Layer 3, or virtual-wire.

Issue Identifier	Issue Description
69458	When a loopback interface is used a GlobalProtect™ gateway, traffic for third-party IPSec clients is not routed correctly. To prevent this issue, use a physical interface instead of a loopback interface as the GlobalProtect gateway for third-party IPSec clients, or configure the loopback interface used as the GlobalProtect gateway to be in the same zone as the physical ingress interface for third-party IPSec traffic.
68588 *This issue is now resolved. See the list of* PAN-OS 6.1.1 Addressed Issues.	Firewalls that are managed by Panorama, but have not been restarted since being configured as managed devices, might forward predefined reports to Panorama that show no data. You can restart the management server for the firewall to ensure that predefined reports are forwarded to Panorama and populated correctly.
68484	On Panorama, if you disable the **Share Unused Address and Service Objects with Devices** setting and perform a device group commit, Panorama does not push all the objects that the firewalls use in policies.
68330	When a WF-500 appliance is configured to generate content updates and a PAN-OS firewall is retrieving incremental content updates from the appliance, the system log shows `unknown version` for the update. For example, after an auto update, the system log shows: `Wildfire package upgraded from version <unknown version> to 38978-45470`. This is a cosmetic issue only and does not prevent content updates from installing.
68153	On a firewall with numerous interfaces, the scheduled and unscheduled (on demand) reports might display discrepancies in the byte counts for traffic logs and the repeat counts for threat and data filtering logs.
67713	PAN-OS is allowing the administrator to downgrade the content version (Applications and Threats) on the firewall to a version that is not supported by the current version of PAN-OS. For example, if the firewall is running PAN-OS 6.1.0 and the minimum content version is 454, the administrator should not be able to downgrade to a version prior to 454.
67624	When using a web browser to view a WildFire Analysis Report from a firewall that is using a WF-500 appliance for file/sample analysis, the report may not appear until the browser downloads the WF-500 certificate. This issue occurs after upgrading a firewall to PAN-OS 6.1 and the WF-500 appliance to version 6.1. Workaround: browse to the IP address or hostname of the WF-500 appliance. This will temporarily download the certificate into the browser. For example, if the IP address of the WF-500 is 10.3.4.99, open a browser and enter `https://10.3.4.99`. You can then access the report from the firewall by selecting **Monitor > WildFire Submissions**, click the log details icon and then click the **WildFire Analysis Report** tab.
66976	In the WildFire submission logs, the email recipient address is not correctly mapped to a username when the mapping is done using group mapping profiles pushed in a Panorama template.
66887	The VM-Series firewall on KVM, for all supported Linux distributions, does not support the Broadcom network adapters for PCI Passthrough functionality.
66879	The VM-Series firewall on KVM running on Ubuntu 12.04 LTS does not support the PCI-Passthrough functionality.
66745	On managed mobile devices running iOS 8, unenrolling the device does not always remove the VPN profile and the Mobile Security Manager profile.

Issue Identifier	Issue Description
66233	When HTTP header logging is enabled in the URL Filtering profile, two issues can be seen: the URL logging rate is reduced or HTTP headers are not logged to the URL Filtering logs when the traffic rate is high. The second issue can cause a delay in receiving headers, resulting in missing HTTP header information.
65824	Unused NAT IP address pools are not cleared after a single commit, so a commit might possibly fail if the cache of unused pools, existing used pools, and the new pools together exceed the memory limit. Workaround: commit a second time, which clears the old pool allocation.
64658	When setting up or modifying a DoS protection profile, you can set a maximum number of concurrent sessions for traffic that matches the DoS profile. The maximum concurrent limit of sessions for the PAN-OS 6.1.0 release is 65,535. Following an upgrade to PAN-OS 6.1.0, check that the **Maximum Concurrent Sessions** you have configured is less than 65,535 (**Objects > DoS Protection > DoS Protection Profile > Resources Protection**). You will not be able to commit configuration changes if the Maximum Concurrent Sessions field was set to a value higher than 65,535 while running a previous release version. Enter a value for this field that is less than 65,535 in order to continue to commit configuration changes following the upgrade.
63962	Configurations pushed from Panorama 6.1 to firewalls running PAN-OS versions 6.0.0 to 6.0.3 will fail to commit due to an unexpected `Rule Type` error. This is because the new **Rule Type** setting in security policy rules was not included in the upgrade transform and therefore the new rule types are not recognized on the devices.
63524	When you perform a template commit to a PA-200 firewall, the operation fails if you changed the vsys1 display name on the firewall using the CLI command `set display-name <name>`. Workaround: leave the display name at its default value (vsys1) or, if you already changed it, reset it to the default value.
63186	If you perform a factory reset on a Panorama virtual appliance and configure the serial number, logging does not work until you reboot Panorama or run the CLI command debug software restart management-server.
60229	A cached web page maybe accessible to a user, even if the URL category is blocked by policy. However, if the user uses the links on the web page to request additional content from the blocked category, the request will be successfully blocked by policy.
58260	If a HA failover happens on Panorama at the time that the NSX Manager is deploying the NSX edition firewall, the licensing process fails with the error: `vm-cfg: failed to process registration from svm device. vm-state: active`. Workaround: Delete the unlicensed instance of the VM-Series firewall on each ESXi host and then redeploy the Palo Alto Networks NGFW service from the NSX Manager.
49322	After you configure Panorama M-100 appliances for high availability and synchronize the configuration, the Log Collector of the passive peer cannot connect to the active peer until you reboot the passive peer.
40436	PAN-OS does not update FQDN entries unless you enable the DNS Proxy caching option.

PAN-OS 6.1.4 Addressed Issues

The following table lists the issues that are fixed in the PAN-OS 6.1.4 release. For new features introduced in PAN-OS 6.1, associated software versions, known issues, and changes in default behavior, see PAN-OS 6.1 Release Information.

Issue Identifier	Description
78272	Enhancements have been made to the WF-500 WildFire™ appliance to reduce incorrect malware verdicts for PDF files.
78206	Fixed an issue where a multi-dataplane platform did not properly free SSL forward proxy memory for SSL session-cache entries that included a username field that was parsed from a client certificate. With this fix, memory is freed up as expected for session-cache entries that include a username field parsed from a client certificate.
77707	Fixed an issue in PAN-OS 6.0.9 where **Threat Map** and **Traffic Map** were not appearing on the web interface under **Monitor > App Scope > Threat Map** or under **Monitor > App Scope > Traffic Map**.
76615	Fixed an issue where running the `request system private-data-reset` command when there was a faulty disk drive on the Log Processing Card (LPC) caused an LPC failure during reboot.
76570	Fixed an issue where a commit failed when uppercase-to-lowercase transformation of group and user configuration objects was not performed uniformly for all objects. With this fix, all uppercase group and user configuration objects are transformed to lowercase characters as expected during configuration parsing.
76561	Fixed an issue where the DHCP relay agent dropped DHCPDISCOVER packets that the agent could not process due to multiple BOOTP flags. With this fix, the DHCP relay agent recognizes the first BOOTP flag in a DHCPDISCOVER packet and ignores any additional BOOTP flags that may exist (per RFC 1542) so that multiple BOOTP flags do not cause DHCPDISCOVER packets to be dropped.
76238	A security update was made to address CVE-2015-1873.
76185	Fixed a rare issue where both devices in a high availability (HA) active/active configuration entered active-primary state when the two firewalls completed the boot process almost simultaneously.
76110	Fixed an issue where error logs were generated for failed network time protocol (NTP) sync events even though there was no NTP server configured on the firewall. With this fix, error logs no longer include false failure messages for NTP sync.
76099	Fixed an issue where the dataplane restarted on a PA-7050 firewall when there was a NAT rule configured to use dynamic IP that falls back to dynamic IP and port (DIPP) NAT.
76043	Fixed a memory allocation issue on the PA-7050 firewall that caused intermittent connectivity for sessions inspected using SSL Forward Proxy decryption. An update was made to increase the proxy memory pool for PA-7050 firewalls, to allow for more memory to be allocated for SSL Forward Proxy sessions.

Issue Identifier	Description
76007	Fixed an issue where an asymmetric path configured with the **drop packet** option no longer worked as expected after an upgrade to a PAN-OS 6.1 release from an earlier PAN-OS feature release (PAN-OS 6.0 or earlier).
75905	Fixed an issue where a firewall failed to download the BrightCloud database via proxy after upgrading to PAN-OS 6.0.8.
75783	Fixed an issue where GlobalProtect™ agent software failed to upload successfully to Panorama. With this fix, you can successfully upload and save the GlobalProtect agent file to Panorama (**Panorama > Device Deployment > GlobalProtect Client > Upload**) and then activate the **GlobalProtect Client** using that file (**Activate From File**).
75740	Fixed an issue where the log-receiver crashed during a restart that happened at the same time that a NetFlow profile was removed from a security rule that was still processing traffic.
75701	Fixed an issue where values for data displayed in Network Monitor charts (**Monitor > App Scope > Network Monitor**) changed from kilobytes and megabytes (KB/MB) representation to bytes after upgrading to PAN-OS 6.1. With this fix, data displayed in charts is displayed using KB/MB values.
75534	Fixed an issue where the reportd process crashed when executing the `show query result id <last job id> skip 0` command.
75103	Fixed an issue where user was not notified of a commit failure when exceeding the maximum number of policy-based forwarding (PBF) rules in the configuration. With this fix, an error will be displayed as expected if trying to commit a configuration when the number of PBF rules exceeds the maximum allowed limit.
74932	Fixed an issue where high availability (HA) failovers that occurred with simultaneous route advertisements caused a routing process to restart, which then caused the firewall to restart.
74914	Fixed an issue in an asymmetric path configuration where HTTP GET requests were successful even though the session matched a custom URL category configured with the **block-url** action. In addition to this fix, you must permit asymmetric traffic in your environment for the block page to display when expected: • Configure a Zone Protection profile with the **Asymmetric Path** set to **bypass** (**Network > Network Profiles > Zone Protection > Packet Based Attack Protection > TCP Drop**) and apply the profile to the ingress zone for the asymmetric traffic; or • Enable asymmetric bypass globally on the firewall with the following configure mode CLI command: `set deviceconfig setting tcp asymmetric-path bypass`.
74735	Fixed an issue where a PA-7050 dataplane restarted when attempting to process jumbo frame packets.
74511	Fixed an issue where static discard routes did not get redistributed using OSPF; the routes were not injected in the OSPF link-state database (LSDB). With this fix, static discard routes are injected into the LSDB and distributed using OSPF as expected.

Issue Identifier	Description
74506	Fixed an issue where, in some cases after selecting **5** (default) in the **Context** drop-down of the **Config Audit** tab (**Device** (or **Panorama**) > **Config Audit**) and clicking **Go**, the web interface returned the `Preparing config audit results` message and then stopped responding. To work around this issue in PAN-OS 6.1.3 and earlier releases, close the web interface and log in again and, if performing another Config Audit, choose a Context value other than **5**.
73878	Fixed an intermittent issue where BGP failed to redistribute the static discard routes as expected after a high availability (HA) failover.
73712	Fixed an issue where viewing the traffic map for outgoing traffic in the Application Command Center (ACC) displayed data using the **source country** filter instead of the **destination country** filter. With this fix, viewing outgoing traffic in the Traffic Map is correctly filtered using **destination country**.
73710	Fixed an issue where, in some circumstances, tags learned via a VM Information Source failed to be removed from an IP address on the firewall when a VM information source indicated that the tag needed to be removed.
73689	Fixed an issue where traffic interruptions occurred due to nested encoding (ZIP content within chunked encoding), which caused the `SML VM vChecks` buffer pool to overflow. With this fix, new checks have been added to prevent `SML VM vChecks` buffer leaks.
73605	Fixed an issue where the User-ID process became unresponsive when trying to acquire the same lock twice with the same thread while executing the `idmgr reset` command for type `user`.
73598	Fixed an issue where executing the `show resource limit session` command displayed `max session` as `0` even though the device had the default configured for maximum number of sessions supported on the firewall.
73481	Fixed an issue where a user with Admin Role permissions was unable to download a PDF file of the App Scope report (**Threat Monitor > App Scope**).
73197	Fixed an issue where the `domain is invalid` error message was displayed when attempting to add a new domain to the LDAP server configuration (**Device > Server Profiles > LDAP**) when the domain name included special characters. With this fix, the LDAP Server profile accepts special characters for NetBIOS domain names.
73152	Fixed a rare issue where 0-byte traffic logs were unnecessarily generated on a PA-7050 firewall for failed attempts to establish a dynamic IP NAT session when the IP pool was running low on IP addresses during heavy traffic flow. With this fix, the unwanted 0-byte logs are no longer generated.
73116	Fixed an issue where a firewall was unable to fetch an external block list (EBL) that included a truncated URL in the HTTP GET request (URL was truncated due to special characters in the original URL). With this fix, URLs with special characters in the EBL successfully upload to the firewall (**Objects > Dynamic Block Lists**) and are accessible for use in security rules.

Issue Identifier	Description
73060	Fixed an issue where web sites that were added to the list of cached servers excluded from decryption were incorrectly added to the list using the IP address and port of the SOCKS proxy when the firewall was between the clients and the proxy server. This issue disabled decryption for all subsequent sessions passing through that proxy server. With this fix, the actual hostname of the web site to be excluded is added to the exclude-cache list and traffic to sites not listed in the exclude-cache list continue to be decrypted as expected.
73058	Fixed an issue where source and destination fields in SNMP traps were not populated for traffic using IPv6 addresses. With this fix and Rev. B of the PAN-OS 6.1 Enterprise SNMP MIB modules, new IP version-neutral fields were added (InetAddress and InetAddressType in place of the IpAddress field) to fully support IPv6 addresses. (The IpAddress field is retained for backward compatibility but is deprecated; administrators are expected to transition to the new fields.)
72820	Fixed an issue on a PA-7050 firewall where a memory leak was observed related to the First Packet Processor (FPP) management plane process.
72811	Fixed an issue on PA-500 firewalls where an unexpected refresh date and time was displayed for the dynamic block list when executing the `request system external-list show name` CLI command. With this fix, the correct time and date are displayed for the dynamic block list.
72801	Fixed an issue where no warning was issued for an interface configured with an invalid OSPF authentication profile. With this fix, an `authentication is invalid` error message is displayed when the name of an OSPF authentication profile has changed and needs to be updated for an OSPF interface (**OSPF > Area > Interface**).
72715	Fixed an issue where Panorama failed to acknowledge and display logs that were forwarded from managed firewalls after upgrading to Panorama 6.1.2 or Panorama 6.1.3. To work around this issue when running either of these two releases, add the firewalls as **Collector Group Members** of a collector group in Panorama (**Panorama > Collector Groups > Device Log Forwarding**).
72665	Fixed an issue where custom reports (**Monitor > Manage Custom Reports**) that use summary logs as their data source display only one report per calendar day (labeled with `23:00`) when output is grouped by **hour**. In PAN-OS 6.1.3 and earlier releases, you can work around this issue by using traffic logs as the data source.
72119	Fixed an intermittent issue on VM-Series firewalls where GlobalProtect clients stopped connecting and displayed a `Connection Failed` error, possibly due to an `encap/decap context` leak. With this fix, the `encap/decap context` leak is no longer observed.
71940	Fixed an issue where the dataplane restarted when SSL Inbound Inspection was enabled due to a software buffer overflow condition. With this fix, the software buffer size is increased to avoid this overflow condition.
71934	Inline editing is supported only for objects that do not include complex fields (fields that can contain more than one value). You must use dialog editing to successfully modify objects that include one or more complex fields so this fix disabled inline editing for objects, such as Redistribution profiles, that contain complex fields. Inline editing is still available for objects that contain only simple fields (those that contain only simple values, such as a single string or integer).

Issue Identifier	Description
71828	Fixed an issue where the management plane ran out of memory due to stalled processes related to exporting logs. With this fix, the schedule log export jobs complete as expected.
71692	Fixed an intermittent issue where some nested user groups did not display in the **User Groups** window (**Device > Local User Database > User Groups**) due to missing short name values that are used to display the groups. With this fix, nested user groups retain their short name value and are displayed as expected in the **User Groups** window.
71611	In response to an issue on PA-7050 firewalls where logs did not always get generated or forwarded as expected when DNS response times were too slow, the `debug management-server report-namelookup` CLI command was added. If you are unable to correct DNS server issues to improve response time on your network, use the `debug management-server report-namelookup` command to work around this issue by disabling DNS name lookups in reports.
71609	Fixed an issue where attempts to add an email address (**Device > Server Profiles > Email**) that included any special characters resulted in an `<email address> is invalid` error message. With this fix, you can add email addresses that contain special characters in the local portion of the address (in front of @) as specified in RFC 3696.
70919	Fixed an issue where the dataplane in a high availability (HA) active/active configuration restarted when a `session update/remove` message was received from the peer while the session was pending an FPGA result. With this fix, FPGA results are ignored if the system receives a `session update/remove` message while waiting for those results.
70719	Fixed an issue where a dataplane restarted due to an incorrect flow ID. With this fix, additional checks are in place to prevent the dataplane from restarting due to this issue.
70669	Fixed an issue where the User-ID process stopped responding due to bulk and incremental updates of terminal server users on the active-secondary device in a high availability (HA) active/active configuration.
70523	Fixed an issue where coverage information in a WildFire Analysis report displayed conflicting information for WildFire and content coverage. With this fix, columns are updated so that the Date Released column displays the date a WildFire signature was first released and the Content Version column is renamed to Latest Content Version and displays the most recent content release version containing that particular signature.
70431	Fixed an issue where a custom URL category with the name any caused unexpected results. With this fix, the name any is no longer allowed when creating a custom URL category (**Objects > Custom Objects > URL Category**).
69959	Fixed an issue where a shared gateway was missing from the drop-down when specifying an Action in the **Forwarding** tab of a **Policy Based Forwarding Rule** (**Policies > Policy Base Forwarding**) after upgrading from PAN-OS 4.1 to PAN-OS 5.0 or higher releases. The missing gateway was not available via the CLI, either. With this fix, all shared gateways used when specifying a forwarding action are preserved during the upgrade.
69837	In response to a rare issue where a PA-200 firewall stopped processing traffic, additional troubleshooting information and some modifications to error checking and counter processes were added to help prevent this event and identify the root cause if it reoccurs.

Issue Identifier	Description
69802	Fixed an issue where the window that popped up when clicking **Browse** to select an **Address** for an **Address Object** (**Objects > Address Groups > Address Group**) could not be resized. With this fix, the Browse window can be resized as needed.
69649	Fixed an issue where an HA3 interface was displayed in the web interface on PA-7050 firewall in high availability (HA) active/passive mode. With this fix, the HA3 interface appears only in an active/active HA configuration as expected.
69543	Fixed an issue where only output for the first virtual system (vsys) was displayed for a configuration with multiple virtual systems when a vsys administrator with access rights to multiple virtual systems executed the `show arp all` command. With this change, a vsys administrator can correctly view the ARP table for the vsys specified in the `set system setting target-vsys` CLI command.
69324	Fixed an issue where a Log Collector group configured with local as the group name triggered a reboot loop. With this fix, local is no longer allowed for use as the name of a Log Collector group.
69131	Fixed an issue where, on certain platforms, a commit job that was pushed when the management plane CPU was under heavy load caused the firewall to restart. With this fix, the commit process is modified to prevent it from causing a service interruption regardless of the CPU load at the time the commit is pushed.
68559	Fixed an issue where a URL containing other embedded URLs with encoding (such as a redirect notice) that was encountered during the Captive Portal authentication process caused a loop in the web browser that required the browser to be closed and restarted. With this fix, Captive Portal properly handles these URLs.
68557	Fixed an issue where a dataplane stopped responding when zeroes were added before the session ID when running the `show session all start-at <session-id>` command.
67458	Fixed an issue where a dataplane failed to get IP pool information from a dynamic IP and port (DIPP) source network address translation (SNAT) rule with an interface IP address.
66406	Fixed an issue where the current application version was not displayed correctly for managed firewalls when the firewall did not have a Threat Prevention subscription.
59914	Fixed an issue where the firewall did not remove the pan_task_x.log or .log.old files as expected when executing the `debug dataplane packet-diag clear log log` command.

PAN-OS 6.1.3 Addressed Issues

The following table lists the issues that are fixed in the PAN-OS 6.1.3 release. For new features introduced in PAN-OS 6.1, associated software versions, known issues, and changes in default behavior, see PAN-OS 6.1 Release Information.

Issue Identifier	Description
75869	Fixed an issue where the dataplane on a PA-5000 Series firewall running PAN-OS 6.1.2 stopped responding when processing encapsulated traffic.
74663	Fixed an issue where a static address group that exceeded the 500 address-object limit caused the dataplane to restart when trying to commit after a push from Panorama. With this fix, a commit that is pushed from Panorama and includes more than 500 address objects in a static address group will fail with a limit constraint error rather than restart the dataplane.
74526	Fixed an issue where the members listed by the `show user group name` command failed to include members of nested groups when using LDAP to connect to a lightweight directory service (LDS) active directory (AD) with **LDAP Server Settings Type** set to **other** (**Device > Server Profiles > LDAP**). With this fix, all members are listed as expected when connected to LDS with **LDAP Server Settings Type** set to **other**.
74212	Fixed an issue where an administrator with superreader access could no longer access `set password` and `set cli` commands in Operational mode after an upgrade to PAN-OS 6.0 and PAN-OS 6.1 release versions. With this fix, superreader administrators can execute these `set` commands in Operational mode.
74187	Fixed an issue where a web browser stopped responding when trying to access a URL where the admin override password was configured but the password value was `NULL`. With this fix, the firewall returns an appropriate failure message if receiving a `NULL` value for admin password override.
74138	Fixed an issue where PA-7050 firewalls in high availability (HA) mode experienced packet buffer leaks in PAN-OS 6.0 or higher releases. One instance of this issue occurred when the interface tables on two HA devices were out of sync and HA session sync messages included an interface ID that did not exist on the receiving device. Another instance was when the interface configurations on two HA devices did not match.In a third instance, a packet buffer leak occurred when the interface IDs on the two firewalls did not match even though the same set of interfaces were configured on the HA devices. This issue also occurred during an upgrade from PAN-OS 6.0 to PAN-OS 6.1 due to interface ID mismatch during the period where two firewalls in an HA pair are not running the same software version. With this fix, packet buffer leaks caused by such interface ID mismatch are prevented.
74049	Fixed an issue where the dataplane intermittently restarted on a PA-5000 Series firewall under heavy load conditions. This fix raises the priority of system health monitor packets so that they do not get dropped and cause the device to restart when under a heavy traffic load.

Issue Identifier	Description
73813	When using the PAN-OS CLI in configuration mode, the CLI command `show predefined signature` incorrectly displayed App-ID signatures and patterns for some predefined applications. The `signature` command option has been removed and the command `show predefined` now correctly displays application information, but does not display the App-ID signature and pattern.
73690	Fixed an issue where entering the `clear session all filter application dns` command on one dataplane incorrectly cleared the web-browsing session on the other dataplane. With this fix, the `clear session all filter application dns` command clears DNS sessions only on the dataplane on which the command is executed.
73630	Fixed an issue where an internal communication failure occurred when an internal virtual router interface tag (VR-ID) was updated while executing the `debug device-server reset id-manager type` command but the DHCP client and server were unaware of the change. With this fix, the DHCP client and server are aware of the VR-ID change and resolve the communication fault.
73337	Fixed an issue where a VM-Series firewall with a VPN configuration restarted due to a buffer overflow caused by a race condition.
73309	Attempting to use the web interface or CLI to upload a WildFire™ content release to Panorama displayed an error (**Device > Dynamic Updates > WildFire**). This issue has been fixed so that WildFire content updates can be uploaded successfully to Panorama.
73193	Fixed an issue where system, config, and threat (except URL) logs were forwarded to a syslog server as expected but traffic and URL threat logs were no longer forwarded after an upgrade from a PAN-OS 6.0 release version to a PAN-OS 6.1 release version. With this fix, all logs are forwarded to the syslog server as expected.
73180	Fixed an issue where, with Strip X-Forwarded-For (XFF) enabled under **Device > Setup > Content-ID**, an X-Forwarded-For IP address was not stripped before the packet was forwarded because the XFF header was split into two TCP segments due to an unusually long HTTP GET request. With this fix, the XFF field is stripped as expected when the header is split across two or more packets.
73109	Fixed an issue where an incorrect port mapping configuration caused packet loss on a PA-3060 firewall configured with Aggregated Ethernet (AE) interfaces 3 and 4.
73089	Fixed an issue where sender and recipient email addresses for some SMTP and POP3 sessions were not captured in WildFire Submission logs.
73071	Fixed an issue where the firewall incorrectly sent duplicate SYN packets for ftp-data sessions.
73068	Fixed an issue where a warning for application dependencies was displayed when committing a new or modified interzone security policy. With this fix, interzone security policy changes do not trigger the application dependency warning when committing configuration changes.
73045	Fixed an issue where the configuration daemon restarted while editing the candidate configuration, causing uncommitted changes to be lost.

Issue Identifier	Description
73017	Fixed an issue where an autocommit failed on firewalls managed by Panorama running a PAN-OS 6.1 release version after upgrading the firewalls from a PAN-OS 5.0 release version to a PAN-OS 6.0 release version.
72915	Fixed an issue where attempts to change the virtual system (vsys) configured for a virtual router (**Network > Virtual Routers**) failed when the Language Preference in the web interface was set to Japanese.
72897	Fixed an issue where a change to the IP address for an interface address object (**Objects > Addresses**) did not display properly for VPN and routing use (**Network > Interfaces**).
72859	Fixed an issue where some threat logs did not display the correct direction for some entries after upgrading to PAN-OS 6.0 or 6.1 release versions when policy-based forwarding (PBF) was configured. With this fix in PAN-OS 6.1.3, the transmission direction for threat log entries is reported correctly when PBF is configured.
72825	Fixed an issue where traffic interruptions for various traffic patterns occurred when data was not released after packet processing. This caused Vchecks to remain allocated for an extended period of time, which depleted the buffer pool. With this fix, the Vcheck offset is modified so that data can be released and processed at a later time and avoid traffic interruptions.
72763	Fixed an issue where HA3 packet forwarding failed in a high availability (HA) active/active configuration when using an Aggregate Ethernet (AE) subinterface to send and receive traffic.
72741	Fixed an intermittent loss of DNS traffic that occurred when the second of two UDP packets was dropped if it arrived at the firewall immediately after the first packet and before the UDP session could be established. With this fix, the new UDP session is created before the second packet is processed so packets are not dropped.
72737	Fixed a memory corruption issue that caused the dataplane to restart when SSL decryption was enabled.
72730	Fixed an issue where it was possible for a firewall under heavy load conditions to send malformed BGP keep-alive messages to a BGP neighbor, causing the BGP neighbor to flap.
72662	In response to an issue where a web server process stopped responding, a check was added to help prevent further instances of this issue.
72582	Fixed an issue where a Scheduled Log Export failed when FTP was specified and the password included special characters (**Device > Scheduled Log Export**). With this fix, special characters in passwords can be used when configuring a Scheduled Log Export using FTP.
72536	Fixed an issue where packet buffers leaked when a firewall that had SSL Inbound Inspection enabled attempted to block a connection and send TCP RST packets to the connection endpoints. With this fix, TCP RST packets sent by the firewall to the connection endpoints no longer cause buffers to leak when SSL Inbound Inspection is enabled.

Issue Identifier	Description
72532	In response to an issue where a high availability (HA) active node changed to a non-functional state and returned a `path monitor failure` error, the internal-path-monitor mechanism now includes Ocelot register output when a path monitor failure is detected.
72092	Addressed an LSVPN issue where routes advertised by GlobalProtect™ satellites were not installed in a GlobalProtect gateway routing table. This issue has been resolved so that the GlobalProtect gateway correctly accepts routes from GlobalProtect satellites.
71326	Fixed an issue where entering the `debug user-id clear registered-ip all` command in shared mode (accessed by executing the `set system setting target-vsys none` command, where `none` specifies all virtual systems) did not clear all registered IP addresses from all virtual systems. The workaround for this issue requires executing the command one time for each virtual system. With this fix, execute the `debug user-id clear registered-ip all` command in shared mode one time to clear all registered IP addresses in all virtual systems.
71262	When two M-100 appliances were in a high availability (HA) active/passive configuration, memory usage for the passive appliance increased significantly compared to the memory usage for the active appliance. This was due to a management process memory leak on the passive device and the issue is fixed.
71040	Resolved an issue that caused SFP+ ports to hang following a restart and the ports continued to stay in down state.
70996	When Panorama was used to manage a firewall with a single virtual system, an email Server Profile created by an administrator with the Device Groups and Templates role was stored in the **vsys1** location. When this email Server Profile was referenced in a Log-Forwarding Profile within a specific Device Group, the Device Group commit failed with an invalid reference error. With this fix, when an administrator with the Device Groups and Templates role creates an email Server Profile, the profile is saved in the **Shared** location on Panorama instead of **vys1** and the Device Group commit is successful.
70902	Fixed an issue where importing a certificate into Panorama failed when the certificate file name included a space. With this fix, certificates with a space in the file name are successfully imported into Panorama.
70887	Fixed an issue where clicking the **More** link to view the registered IP address under **Object > Address Groups** resulted in an error if the name of a Dynamic Address Group included a space. With this fix, spaces in Dynamic Address Group names no longer cause an error when displaying the IP address.
70816	Fixed an issue where an `Invalid syntax` error (`not a valid source IP address`) was displayed when running certain commands (`clear session all`, `set application dump`, `test decryption-policy-match`) after initiating a filtering session based on an IPv6 address. IPv6 address validation now works correctly.
70544	A dataplane restart occurred when the SSL Decryption Opt-out Page was enabled (to notify users that SSL connections are decrypted), the RC4 cipher was enforced, and a long URL was accessed. This issue has been fixed so that the dataplane does not restart when the SSL Decryption Opt-out Page is enabled.

Issue Identifier	Description
70304	Resolved an issue where a race condition could occur if new security policies were matched to existing sessions when Rematch Sessions (**Device > Setup > Session**) was enabled.
70295	Fixed an issue where a commit failed when an aggregate subinterface with DHCP client enabled was used for an IKE gateway configuration (**Network > Network Profiles > IKE Gateway**).
70075	Fixed an issue where a lack of content resources on a PA-3000 Series firewall caused some applications to be incorrectly identified or even fail. This fix ensures adequate resources are available for identifying and supporting all traffic sessions.
70036	Fixed an issue where the web interface displayed partial or no results for report requests. With this fix, report requests are completed properly and results are displayed as expected.
69900	Fixed an issue where the tech support file did not contain some expected files, including /var/log files.
69409	Fixed an issue where a security policy containing two nearly identical rules (the only exception that the first rule contained a custom URL category with no specified URLs) prevented some applications from matching the appropriate rule. With this fix, applications match the correct rules and security policies are enforced as expected even if an empty custom URL category is added to a rule.
69266	Fixed an issue where queries were not saved when clicking **OK** when configuring Botnet reports after an upgrade to PAN-OS 6.0 and PAN-OS 6.1 release versions. With this fix, queries built under **Monitor > Botnet > Report Setting** in the web interface are saved when clicking **OK** and filters work as expected when running the Botnet report. As a workaround, you can build the desired query in the web interface but, before clicking **OK**, copy the query text and enter it in the CLI using the `set shared botnet report query` command (the query then displays as a saved query in the web interface).
69242	When a user failed to authenticate using the web interface, firewall system logs did not display the user's source IP address. Updates have been made so that a failed authentication on the web interface is logged with two entries. One entry is logged as a `general` event and displays only the username of the user who failed authentication. The other entry is logged as an `auth-fail` event and displays both the username and source IP address for the user who failed authentication.
69178	Fixed an issue where the DNS Proxy service was aborted when the file descriptors for TCP-based DNS request sessions were prematurely closed. With this fix, TCP-based DNS request file descriptors are allowed to age out and be deselected when no longer needed.
68770	Fixed an issue where a working IPSec tunnel would not reestablish after a NAT configuration was removed. With this fix, IPSec tunnels will successfully reestablish in response to the removal of NAT along the IPSec tunnel path.
67930	Fixed an issue where an update to a stale IPv6 neighbor entry caused a dataplane restart.

Issue Identifier	Description
67709	Fixed an issue where a context switch over to a firewall in Panorama followed by a response page import attempt (**Device > Response Pages**) resulted in a failed import and displayed a misleading `Session timed out` error. With this fix, response page import requests after a context switch in Panorama are successful.
67523	Fixed an issue where the second pair of Aggregate Ethernet (AE) interface ports did not stay down when both ports on the first AE interface went down. This issue occurred on a virtual wire (vwire) with two AE interfaces that had link-state-pass-through enabled and where both ports on one AE interface went down. With this fix, when both ports on one AE interface go down, the second AE interface ports go down and remain in powered down state until the first AE link recovers.
67515	Fixed an issue where clicking the **OK** and **Cancel** buttons did not result in the appropriate action when responding to an error message received after attempting to create an address object with the same name as an existing address object (**Objects > Addresses**). With this fix, clicking the **OK** or **Cancel** button in response to the error message works as expected; clicking **OK** allows the user to continue the process and choose a different name while clicking **Cancel** exits the address object creation process.
67029	Fixed an issue where a large number of `ifInErrors` incorrectly warned of hardware issues after an upgrade to PAN-OS 6.0 or PAN-OS 6.1 release versions. Received counters now correctly differentiate between errors to avoid misleading warnings about hardware.
66113	Fixed an issue where adding a large number of groups and users to the allow list in the authentication profile resulted in longer than expected commit times. With this fix, the time it takes to commit changes to the configuration is reasonable even when an allow list contains a large number of groups and users.
65553	The option to **Highlight Unused Rules** did not work as expected for NAT policies. The expected behavior is for rules that are not being matched to traffic to show as highlighted; in this case, a rule that was not being matched to any traffic was not displayed as highlighted. This has been fixed so that NAT rules that do no match to any traffic are correctly shown as highlighted (**Policies > NAT**).
64887	Fixed an issue on a PA-7050 firewall where some traffic was dropped after a configuration commit that included a change to the interface configuration. With this fix, the firewall updates current available memory as expected when changes to the interface configuration are committed. Without this fix, you can work around the issue by committing a security policy change following any commit that includes changes to the interface configuration, which prompts the firewall to update current available memory settings.
62375	The GoDaddy root certificate authority (CA) was missing from the list of trusted certificate authorities. When SSL decryption was configured, sites using the GoDaddy root certificate authority were displayed as not trusted. With this fix, the GoDaddy Root Certificate Authority - G2 is included in the list of trusted CAs.

PAN-OS 6.1.2 Addressed Issues

The following table lists the issues that are fixed in the PAN-OS 6.1.2 release. For new features introduced in PAN-OS 6.1, associated software versions, known issues, and changes in default behavior, see PAN-OS 6.1 Release Information.

Issue Identifier	Description
73790	Additional security-related enhancements were made to support frame-busting for the firewall web interface, in order to prevent framing of web interface elements.
73757	A security-related fix was made to enforce character encoding specified in HTTP headers due to CWE-116: Improper Encoding or Escaping of Output.
73638	A security update was made to address issues related to HTML encoding.
73594	When you extracted the image for the VM-Series NSX edition firewall from the zip file, the VF/DVMK were labeled ESX instead of NSX. This naming error has been fixed.
73111	Dataplane restarts were caused by a race condition between dataplane packet processes, where the session resource allocation became out of sync between central processing units (CPUs). A fix was added to keep session resource allocation in sync between dataplane processes.
72658	Japanese characters were not displaying correctly when the **App Scope Summary** was exported as a PDF. This issue has been fixed so that exporting a PDF of the **App Scope Summary** page displays characters correctly when the language preference is set to Japanese.
72544	Addressed CVE-2014-8730. For additional information, refer to the PAN-SA-2014-0224 security advisory on the Palo Alto Networks Security Advisories web site at https://securityadvisories.paloaltonetworks.com.
72241	Following an upgrade, attempting to perform a high availability (HA) configuration sync between two HA peers in an active/passive or active/active deployment did not sync correctly. This issue has been fixed so that HA peers will sync correctly following an upgrade.
72115	When the web interface was set to display in any language other than English, service routes to specify how the firewall communicates with other servers or devices could not be configured (**Device > Setup > Services > Service Route Configuration**). This issue has been fixed so that service routes can be configured and work correctly when the web interface is set to any language preference.
72068	If a firewall with Open Shortest Path First (OSPF) enabled was then restarted, a flapping condition was seen between the firewall and the adjacent OSPF neighbor, and a new OSPF election was forced for the firewall. This issue has been fixed so that following a firewall restart, any OSPF adjacency remains established.

Issue Identifier	Description
71951	After restarting a PA-7050 firewall, a longer than expected period of time was necessary for an autocommit to complete and for the firewall to begin passing traffic. This issue was seen when the PA-7050 firewall had a large number of interfaces and address objects configured. An enhancement has been made to speed up the restart process.
71939	Addressed an issue where enabling a second Network Processing Card (NPC) on a PA-7050 firewall resulted in URL packets being dropped by the second NPC and URL lookups could fail. This issue has been fixed so that URL lookups are performed correctly and web pages load quickly.
71893	When a custom URL category was selected as matching criteria for a QoS policy, other traffic besides that defined in the custom URL category was receiving QoS treatment. This has been fixed so that when a custom URL category is configured in a QoS policy, only the websites in that category receive QoS treatment.
71861	A passive device in an HA setup configured with Link Aggregation Control Protocol (LACP) interfaces was generating logs showing link states every five minutes. This issue has been resolved so that devices in a passive, suspended, or non-functional state do not generate logs.
71850	Changing the IP address for a log card interface on a PA-7050 firewall caused an issue where traffic log forwarded to syslog servers stopped until the firewall was restarted. This was due to an issue where the firewall sent out traffic using an internal IP address (which was recognized as an invalid source IP by devices intermediate to the firewall and the syslog server) following a change to the log card interface IP address. This issue has been fixed so that changing the IP address for a log card interface does not cause the firewall to send out traffic using an internal IP address.
71688	On a PA-7050 firewall with OSPF enabled, a restart caused OSPF neighbor adjacency states to flap. This issue was caused by an incorrect slot number setting on the Network Processing Card (NPC) for the session owner. With this fix, the NPC slot number for the session owner is properly selected and OSPF neighbor adjacency is established.
71634	Enhancements have been made to the WildFire™ appliance to reduce incorrect malware verdicts for Shockwave Flash (SWF) files, that were sometimes seen after upgrading the appliance and the firewall to PAN-OS 6.1 releases.
71604	When an SNMP server polled the firewall, the status for interfaces that were not configured was shown as up. An SNMP poll now correctly shows the status for interfaces that were not configured as down.
71553	Fixed an issue where dataplane processes restarted when handling SSL Decryption sessions during high availability (HA) message updates. The fix for this issue included the addition of a global counter.
71521	Addressed an issue where back-end process restarts caused the dataplane to restart. This was due to recursive functions consuming too much stack memory, making it possible for a certain traffic pattern (single byte HTTP chunked encoding) to result in a restart.
71512	A fix was made to add frame-busting to the firewall web interface to prevent framing of web interface elements.

Issue Identifier	Description
71503	Addressed an incorrect file permissions issue in the web interface.
71486	A security-related fix was made to address an issue with user input sanitization to prevent Cross-Site Scripting (XSS) attacks against the web interface.
71464	If a client initiates a Point-to-point protocol over Ethernet (PPPOE) session, an issue was seen when a server responds to the client with a PPOE Active Discovery Offer (PADO) packet that was greater in size than the maximum transmission unit (MTU) of the firewall interface. In this case, the PADO packet was dropped. This issue has been addressed so that PADO packets are handled correctly by the firewall, including when the size of the packet is greater than the MTU for the firewall interface.
71408	An error was displayed on the WildFire portal when downloading a WildFire Analysis Report as a PDF. This issue has been fixed so that using the option to download a WildFire Analysis Report as a PDF works correctly and does not display an error.
71333	In a high availability (HA) active/active configuration with an IPSec tunnel configured to terminate on a floating IP address, Encapsulating Security Payload (ESP) was performed by the device that did not own the floating IP address. The encapsulated packets failed the IPSec anti-replay check on the remote end of the IPSec tunnel and were discarded. With this fix, packets are always sent to the owner of the floating IP address to be encapsulated.
71321	Removed support for SSL 3.0 from the GlobalProtect™ gateway, GlobalProtect portal, and Captive Portal due to CVE-2014-3566 (POODLE).
71320	Removed support for SSL 3.0 from the web interface due to CVE-2014-3566 (POODLE).
71273	A security update was made in PAN-OS to address issues related to parsing XML data.
71199	In a Large Scale VPN (LSVPN) setup, a GlobalProtect satellite reconnecting to a GlobalProtect gateway after receiving a different IP address, changed the GlobalProtect routing metrics when installing the gateway access routes into the satellite routing table. With this fix, the original gateway routing priority is restored when the GlobalProtect satellite reconnects to the GlobalProtect gateway with a different IP address.
71148	When attempting to add an address to an address group using the Panorama web interface, filtering for the address returned no results even though the address object did exist and was displayed as configured on the **Objects > Addresses** page. Additionally, filtering for the same address object when attempting to add the address to a security rule displayed different results for the address object name. This issue has been resolved so that filtering for an address correctly displays any configured address objects, and so that address object names are displayed consistently.
70920	License expiration dates are now enforced on all firewalls according to Coordinated Universal Time (UTC), regardless of the time zone configured for the firewall. This update resolves conflicts between local time zones and license expiration dates, specifically addressing conflicts due to the Daylight saving time (DST) transition.
70903	Fixed an issue where SNMP traps from some firewalls were not parsed correctly by the SNMP manager.

Issue Identifier	Description
70837	VM Information Sources with names containing a space character were not handled correctly, and caused VM information retrieval from Amazon Web Services (AWS) to fail. This issue has been fixed so that VM Information Sources configured with a space character used in the Name field are handled correctly (**Device > VM Information Sources**).
70820	Addressed an issue for PA-7050 firewalls, where Real-time Transport Protocol (RTP) predict sessions remained in the Opened session state and did not become an active session. This caused the RTP packets to not merge correctly with the predict session and the packets were dropped if they did not specifically match to an allow policy.
70706	When configured in a high availability (HA) active/passive configuration, an M-100 appliance could not be accessed using the web interface or the command line interface (CLI). In this case, a restart was required to gain access to the appliance. This issue has been fixed so that an M-100 in an HA active/passive configuration can be accessed correctly by an administrator using the web interface or CLI.
70383	When using the Panorama XML API to register an IP address to a Dynamic Address Group on a targeted firewall, an error was displayed that the user was not authorized to perform the operation. This issue has been resolved so that using the XML API to register an IP address to a Dynamic Address Group on the firewall results in the firewall correctly registering the IP address and updating the membership information for the dynamic address group.
70303	When attempting to create a custom spyware signature, using the **Browse** option to browse for and add threats did not correctly open the **Spyware Browser**; instead, selecting **Browse** caused the **Custom Spyware Signature** dialog to close completely (**Objects > Custom Objects > Spyware**). This issue has been fixed so that selecting **Browse** correctly opens the **Spyware Browser**, and you can then select threats from the browser to be added as conditions for your custom signature.
70302	This fix addresses an issue where the autocommit process failed after upgrading a PAN-OS 5000 Series firewall or a PA-7050 firewall to a PAN-OS 6.1 release.
70150	Resolved an issue where Simple Network Management Protocol (SNMP) traps were not correctly sent to the SNMP trap destinations following a software upgrade. This issue is fixed so that SNMP traps are generated and correctly sent to SNMP trap destinations after performing an upgrade.
69934	Fixed an issue where an active File Transfer Protocol (FTP) connection failed when enabled with Source Network Address Translation (NAT) using a dynamic IP pool. This issue was due to the FTP control channel and the FTP data channel using different source IP addresses and the following error was displayed for the client: `500 Illegal PORT command`.
69737	On platforms with multiple dataplanes, stale IPv6 neighbor entries were not removed and replaced with new IPv6 neighbor entries when the IPv6 neighbor table threshold was reached. This issue has been fixed so that stale IPv6 neighbor entries are correctly removed when the table threshold is reached. Additionally, for both platforms with multiple dataplanes and platforms with a single dataplane, once the table threshold of 70% is reached, a check is now made every 20 minutes to remove entries which have been stale for more than 10 minutes (this check was previously performed every hour).

Issue Identifier	Description
69528	A fix was made so that in an environment where two virtual systems are configured as User-ID collectors for each other, and with captive portal enabled, IP address to username mappings are correctly refreshed among the virtual systems. The fix ensures that users are correctly prompted with the captive portal web page following a timeout.
69191	Addressed an issue where simultaneous downloads of the GlobalProtect installation program caused SSL-based VPN to fail.
68812	In a Large-Scale VPN (LSVPN) configuration, where a GlobalProtect gateway and satellite resided behind a NAT device, the satellite incorrectly attempted to send Encapsulated Security Payload (ESP) packets to the original IP address configured as the gateway interface instead of to the external gateway specified in the satellite configuration for the GlobalProtect portal (**Network > GlobalProtect Portal > Satellite Configuration**). In this case, the ESP packets could not reach the gateway and tunnel traffic failed. With this fix, the GlobalProtect satellite correctly sends ESP packets to the external gateway specified for the satellite in the GlobalProtect portal configuration.
68764	When a proxy server is configured on the firewall, the proxy settings were not used and DNS resolution was requested to resolve service.brightcloud.com. After the fix, the connection request by the firewall to BrightCloud is always forwarded to the proxy.
68560	Addressed an issue where vulnerabilities were logged as unknown when an ampersand character (&) was used in the **Comment** field when creating a custom vulnerability object. Using the ampersand character in the **Comment** field when creating a custom vulnerability object is supported, and does not cause the vulnerability to display as unknown.
68430	The dataplane restarted unexpectedly due to a lack of memory. An update has been made to provide additional debug information for this issue.
68329	An option was added for VM-Series firewalls to provide administrators the capability to change socket buffer depth, in order to accommodate different requirements for packet loss and throughput.
68217	A firewall stopped responding unexpectedly and showed all interfaces as down. To address this issue, Self-Monitoring, Analysis and Reporting Technology (SMART) information is now included in the tech support file and mp-monitor.log file to provide debug information.
67885	Panorama predefined reports for vulnerabilities were inconsistent with the predefined report for vulnerabilities on the managed firewall. This issue has been addressed so that reports are correctly synchronized between Panorama and managed devices.
67861	Following an upgrade to PAN-OS 6.0 releases, virtual wire interfaces went down after restarting the firewall. This issue has been fixed so that the status for virtual wire interfaces is no longer down after upgrading to a PAN-OS 6.0 release and restarting the firewall.
67719	The management interface was not receiving IPv6 connections for traffic from the dataplane when the firewall was in Layer 2 mode. An update was made to the MAC address learning process so that the Management interface receives IPv6 traffic from the dataplane when the firewall is in Layer 2 mode.

Issue Identifier	Description
65553	The option to **Highlight Unused Rules** did not work as expected for NAT policies. The expected behavior is for rules which are not being matched to traffic to show as highlighted; in this case, a rule which was not being matched to any traffic was not displayed as highlighted. This has been fixed so that NAT rules which do no match to any traffic are correctly shown as highlighted (**Policies > NAT**).
62367	On PA-3000 Series firewalls, traffic to and from a Layer 3 interface was failing. Commands have been added to collect further field-programmable gate array (FPGA) information and other debug information for this issue.
61201	Scheduled email reports were not being delivered, though the reports were generating and displaying correctly on the **Monitor** tab on the web interface. This issue was due to a memory leak for a back-end process that maintains configuration information for the firewall. This issue has been fixed so that scheduled email reports are correctly delivered to email.
55249	You can now run the CLI command `test <feature>` for the following features: `botnet, cp-policy-match, custom-url, data-filtering, decryption-policy-match, dns-proxy, dos-policy-match, global-protect-mdm, global-protect-satellite, nat-policy-match, nd, pbf-policy-match, pppoe, qos-policy-match, routing, scp-server-connection, security-policy-match, stats-service, tag-filter, url, url-info-cloud, url-info-host, user-id, vpn, wildfire`.

PAN-OS 6.1.1 Addressed Issues

The following table lists the issues that are fixed in the PAN-OS 6.1.1 release. For new features introduced in PAN-OS 6.1, associated software versions, known issues, and changes in default behavior, see PAN-OS 6.1 Release Information.

Issue Identifier	Issue Description
71618	Dataplane process restarts resulted in a dataplane restart. Improvements have been made to help prevent dataplane processes from restarting.
70588	Fixed an issue that occurred in cases where no client certificate is present; a browser with Transport Layer Security (TLS) 1.2 enforced could not access the GlobalProtect™ portal login page.
70499	Fixed an issue where traffic matched to a predict session and then converted to a flow session was then being incorrectly matched to security policies where the only matching criteria defined in the policy was a custom application. A fix was made to perform a second policy lookup after predict session traffic is converted to flow session traffic.
70459	Addressed an issue where attempting to use the Panorama XML API to request a tech support file for a managed device returned the tech support file for Panorama. An update was made so that an error is displayed if attempting to use the Panorama XML API to retrieve a tech support file for a managed device and the workaround to this issue is to download a tech support file from a managed device directly from the device.
70193	In PAN-OS 6.1.0, a custom HIP check was incorrectly matching to traffic if no processes defined in the custom check's Process List were running on the client system. Custom checks also incorrectly passed (meaning the check did not match to traffic) if all processes defined in the Process List were running on the client system. An update was made so that custom checks are matched correctly to client traffic depending on the status of the processes defined in the Process List: • A custom check does not match to client traffic when all processes defined in the Process List are found to not be running on the client system. • A custom check matches to client traffic when at least one process (or more) defined in the Process is found to be running on the client system.
70165	Fixed an issue for PA-7050 firewalls in a high availability (HA) active/active configuration, where IPv6 fragments could cause a Network Processing Card (NPC) to restart.
70151	The firewall web interface could not be accessed using a Chrome browser following an installation of the Microsoft upgrade KB2998527. This issue has been fixed; as workaround for Chrome, you can also update your Chrome browser to the latest version.
69956	Fixed an issue for PA-5000 Series devices, where NetFlow information for some sessions was not being forwarded due to a session ID format change.

Issue Identifier	Issue Description
69633	An issue was addressed where call forwarding for Voice over IP (VoIP) calls did not work correctly and Real-time Transport Protocol (RTP) traffic was dropped. An update was made to provide further debug information for this issue.
69311	Using the command `scp export log traffic max-log-count <value>` with the `value` variable set to a number greater than 1 million logs was displaying inconsistent results. This was due to the query timeout being 20 minutes, which was not enough time to generate that many logs. The query timeout has been increased to 60 minutes as a fix.
69306	Fixed a misspelling displayed in the help details for the command `request quota-enforcement` in the Panorama command line interface (CLI).
69035	When using the **ACC** tab on the Panorama web interface to view statistics for a custom application, using applications filters (such as the Category, Subcategory, and Technology) to filter the displayed data resulted in no data being displayed. This occurred when Panorama was selected as the **Data Source** for the traffic data displayed on the **ACC** tab, and the issue has been resolved.
68982	Fixed an issue where the firewall stopped receiving new reports from WildFire™ when the report ID on the WildFire public cloud exceeded a certain limit (reports continued to be generated but were not logged on the firewall).
68899	Fixed an issue that affected PA-7050 firewalls. An issue occurred where an HSCI port configured as an HA2 interface went down due to a dataplane board restarting. An improvement has been made so that, if there are more than one dataplane boards up and running, a single dataplane restart will not cause an HA2 interface on an HSCI port to go down.
68885	Fixed an issue that occurred after upgrading Panorama. Administrators that did not have local access, but that were previously authenticated to Panorama, could not log in to the CLI and an error message was displayed.
68836	In a high availability (HA) setup, a path monitoring failure lead to a delayed HA failover. An update has been made to optimize HA failover time.
68768	A base OVF image is available for PAN-OS 6.1. To find the new image, filter by Pan-OS for VMware NSX Base Images on the Palo Alto Networks Support Portal.
68702	An error was displayed when pushing a policy from Panorama to a managed firewall with a user group defined in the policy. The error displayed was `Duplicate group name` and this issue has been resolved so that pushing a user group from Panorama to a managed firewall works correctly.
68588	Predefined reports for a firewall that was connected to Panorama were not being displayed correctly if the firewall had not been restarted since initially connecting to Panorama. This issue has been fixed so that predefined reports for a firewall are displayed correctly after establishing a connection with Panorama.
68528	Modifying a policy rule by removing a **Source User** entry and using the **Any** default for the **Source User** field resulted in a commit failure when attempting to save the changes. This issue has been fixed so that when a source user is removed from a policy rule, the policy rule can be successfully modified to use the default of **Any**.

Issue Identifier	Issue Description
68498	Fixed an issue where a validation error occurred when pushing a service from Panorama to a managed firewall.
68491	Certificates expiring after the year 2050 showed an error for the certificates' validity time field. This was due to an issue where, when decryption was performed on a certificate, the standard field meant to display when the certificate expires (`generalizedTime`) was modified to display a field that is not standard (`utctime`) .This has been updated so that the validity for a certificate expiring after the year 2050 is displayed correctly.
68472	Addressed an issue where some expected counters were not returned in the output for the XML API command `<show> <interface>` for loopback, VLAN, and tunnel interfaces.
68409	When setting up BGP **Import Rules** or **Export Rules**, configuring a **Community Type** as **Append** and then an **Append** value of `AS:0` displayed an error (**Network > Virtual Routers > BGP > Import/Export > Action > Community**). This issue has been fixed to allow the value of the **Append** field to be `AS:0` or `0:N` (`0:0` as a value is not supported).
68389	The Application sub-category is listed as unknown in the PDF report for custom applications pushed from Panorama. This issue was resolved by correcting the report daemon to properly parse the configuration objects pushed from Panorama.
68380	An issue occurred when a device group configuration was pushed from Panorama to a managed device. When the commit failed, neither the Panorama web interface nor the CLI displayed an error message. The web interface continued to display the status `config sent to device` and the CLI showed the failures status of the jobs; however, neither the web interface nor the CLI displayed an error message. A fix was made to display commit errors and details for Panorama and the managed device that did not correctly receive the pushed configuration.
68372	Setting up a static MAC configuration for a tagged interface configured on a VLAN did not work correctly. This was due to an issue where a process that communicates between the dataplane and the management plane restarted, and the issue has been resolved.
68371	Addressed an issue where you could not install the BrightCloud database when the default url-db was set to PAN url-DB, and you had not downloaded the BrightCloud database previously.
68355	For a device in a high availability (HA) active/active configuration, the web interface displayed an incomplete list of the HA virtual addresses configured to be used in the HA active/active cluster—the Virtual Address table displayed only six interfaces with assigned IP addresses when eight interfaces were actually configured. A scroll bar has been added to the Virtual Address table to allow you to scroll up or down to view the complete list of configured HA virtual addresses (**Devices > High Availability > Active/Active Config > Virtual Address**).

Issue Identifier	Issue Description
68320	The Logging and Reporting Settings section on the web interface incorrectly displayed a logarithm for unallocated Log Storage when the total allocated log storage quota was configured to be 100% and unallocated log storage was 0% (**Device > Setup > Management**). This was a cosmetic issue and has been fixed so that **Log Storage** on the **Logging and Reporting Settings** window displays unallocated log storage as 0 MB when log storage is 100 % allocated.
68319	When FIPS mode was enabled, the web interface becomes unresponsive when configuring a GlobalProtect gateway and a browser refresh was required to continue using the web interface. A check was introduced to ensure that the web interface does not become unresponsive when creating a GlobalProtect gateway with FIPS mode enabled.
68286	An issue was seen where setting up a password for a proxy server caused the management plane to restart (**Device > Setup > Services > Proxy Server**). This was due to a backend process restarting when the password was configured and has been fixed.
68100	An issue was resolved where the **Strip X-Forwarded-For Header** option did not correctltly remove an internal IP address (**Device > Setup > Content-ID**).
68055	Mac clients were incorrectly unable to access certain websites that Windows clients were able to access. This issue occurred when fragmented traffic passed through the firewall and the first fragment did not include the header; this caused packets to be dropped. The issue has been resolved.
67864	When a rule pushed from Panorama is selected on a managed device, the **Clone** button in a security policy is enabled; however, rules pushed to a managed device from Panorama cannot be cloned on a managed device. With this fix, the **Clone** button for rules pushed from Panorama correctly shows as disabled on the web interface for a managed device.
67810	When a PA-5000 Series device initiates sessions on different data planes in an environment with multiple virtual systems, sometimes session traffic failed to span across virtual systems. This issue has been resolved so that inter-virtual system sessions succeed with a dynamic network address translation (NAT) policy configuration.
67676	Upgrading Panorama to a major release resulted in Panorama losing connectivity with managed firewalls (a major release is any release where the release number ends in 0, for example PAN-OS 6.0.0 or PAN-OS 6.1.0). This was due to an issue with the log schema file and an update was made to ensure that the log schema file is overwritten during an upgrade, even if the file size is zero.
67567	When a new version of the BrightCloud URL database was downloaded and installed, if there was a change to the category for a URL between the old and the new database, the change was not reflected on the dataplane. With this fix, URL categories on the dataplane are updated correctly after installing a new version of the BrightCloud database.
67516	Fixed an issue with a high availability (HA) active/active configuration where a physical MAC address was returned for a floating IP address instead of a virtual MAC address. This has been addressed so that the floating IP correctly responds to ARP requests with a virtual MAC address.

Issue Identifier	Issue Description
67455	Made an update to the enforcement for the SSL Inbound Inspection setting block when resources are unavailable so that hosts cannot resume an SSL session, when that session has been removed from the SSL-decrypt session cache due to the cache being full. The host must start a new session to continue.
67436	The commands `debug software trace reportd` and `debug software core reportd` were added to the CLI command structure.
67344	Fixed an issue for the M-100 appliance where the `show log-collector detail` command was presenting incorrect information.
67300	Addressed an issue on the VM-Series firewalls where enabling packet capture for certain application-level gateway (ALG) traffic caused the system to restart.
67258	The mprelay process, a process that communicates between the dataplane and the management plane, unexpectedly restarted. A Policy Based Forwarding Rule configured with symmetric return, but not specifying an IPv6 next hop address, resulted in excessive Neighbor Discovery (ND) update messages and caused a conditional loop. This is what lead to the mprelay process restart and has been addressed so that IPv6 ND is performed correctly if no IPv6 next hop address is specified, and does not result in the mprelay process restarting.
67187	The following error was displayed due to an issue that caused a User-ID process to restart: `Abnormal system memory usage detected, restarting userid with virtual memory`. Many GlobalProtect users logging into the system, and the resulting high availability (HA) synchronization of the HIP reports, caused the virtual memory to exceed its limit.
66953	The maximum number of tags that PAN-OS and Panorama support for each virtual system and device group (including the Shared group) is now 2,500 instead of 1,000.
66920	Secure Shell (SSH) traffic was incorrectly categorized as URL Category `unknown`. This has been fixed so SSH traffic is not assigned a URL category.
66630	After changing the domain name setting in an LDAP server profile, users failed to authenticate with the new LDAP server. This was due to a missing function that updates the internal group database name and has been resolved.
66466	Addressed an issue for the PA-2000 platform, where a device failed to handle high volume of packets (larger than the MTU) on the management interface. Symptoms of this issue included device unresponsiveness, a random restart, traffic failures or ATA errors on the console. This issue has been resolved.
66364	Fixed an issue that prevented two certificates with the same subject name from being installed following an upgrade to PAN-OS 6.0.X.
66220	An issue was seen in a high availability (HA) active/passive configuration where the secondary device was not able to pass traffic after a failover until a routing process was restarted. This issue has been fixed so that when a failover occurs, the secondary device correctly becomes the Backup Designated Router (BDR).

Issue Identifier	Issue Description
66073	An issue with the command `debug system ssh-key-reset high-availability` generating a 0 byte key file has been resolved. This issue has been resolved so that the `debug system ssh-key-reset high-availability` command generates valid key files.
66010	The firewall did not resolve FQDNs used in policies when the DNS responses contained Canonical Names (CNAMEs) with capital letters. With this fix, the firewall properly resolves the FQDNs, regardless of the case of the letters in the returned CNAMEs.
65859	Fixed an issue where the dataplane could restart when SSL Forward Proxy decryption was enabled and a certain packet sequence was received.
65850	Addressed an issue where a high availability (HA) backup failed due to there being no buffer space available.
65727	Unexpected traffic loss was seen on PA-5000 Series firewalls. This issue could not be reproduced; an update has been made to provide further debug information to help troubleshoot the issue if it occurs again.
65565	Fixed an issue where selecting Replay attack detection in the GlobalProtect gateway satellite configuration did not actually enable replay attack detection when configured in the web interface.
64930	Dynamic objects could be lost if the device server restarted unexpectedly. This has been fixed so that dynamic objects are repopulated if the device server process unexpectedly restarts.
63150	In a high availability (HA) active/active configuration, User Datagram Protocol (UDP) sessions with a certain traffic pattern caused the session state to flap frequently and generate excessive traffic logs. This issue is now fixed and the session state is stable.
62768	Unreliable DNS servers might incorrectly provide NXDOMAIN responses. To help prevent incorrect WildFire sample categorization, NXDOMAIN responses are no longer shared across WildFire samples. Each NXDOMAIN response will be evaluated on a sample by sample basis.
61205	Using the web interface to export traffic logs in CSV format was showing an error that the query job failed. This issue has been addressed so that exporting traffic logs to CSV works correctly.

PAN-OS 6.1.0 Addressed Issues

For new features, associated software versions, known issues, and changes in default behavior, see PAN-OS 6.1 Release Information.

If you have asymmetric routes in your network, before upgrading to 6.1.0, use the following command to ensure session continuity: `set deviceconfig setting tcp asymmetric-path bypass`. And, if you have attached a zone protection profile, you must also use the following command: `set network profiles zone-protection-profile <profile-name> asymmetric-path [bypass | global]`.

The following is a list of issues that are fixed in the PAN-OS 6.1.0 release:

Issue Identifier	Issue Description
69173	Under certain conditions, unspecified layering of packet-level evasions could be used to bypass signature matching of the session.
68708	Addressed the bash vulnerability CVE-2014-7169 that relates to how environment variables are processed when the shell starts up. This fix prevents a user with an account on the firewall, from using the vulnerability to gain escalated privileges.
67833	While generating a tech support file on Panorama, private information was not being removed correctly from files within a device group if the device group had a space in its name. With this fix, device groups with spaces in their names are handled correctly when generating a tech support file.
67814	Panorama displayed the secure-proxy-password in the web interface under **Panorama > Setup > Services** and in the CLI. With this fix, Panorama encrypts the secure-proxy-password and downgrade attempts to versions which show the secure-proxy-password will fail until you remove the secure-proxy-password from the configuration.
67788	The configuration log on Panorama displayed the secure-proxy-password. With this fix, the configuration log encrypts the secure-proxy-password.
67782	If a policy had more than one tag, and you wanted to filter the policies based on one tag but not the other tag, the logic failed and the filter did not work. With this fix, the filter is working as expected.
67720	The Network Processing Card (NPC) on the PA-7050 firewall continually restarted when link errors were present, causing a system restart to occur. An update to the internal link failure recovery logic now prevents system restarts when link errors are present.
67674	Resolved an issue where a misspelling in a label in the PAN-TRAPS.my MIB file resulted in a failure to load the MIB.
67268	When configuring DNS sinkhole, the firewall was unable to display the IP address of the client that was initiating corrupt DNS requests in the logs. With this fix, the logs display the source IP address of the client.

Issue Identifier	Issue Description
67182	External Block Lists (EBLs) were not properly parsed during the initial load. This caused the load to fail if Windows formatted files were used, where <CR><LF> line feeds were used instead of standard UNIX <LF>. Comments were also not properly supported on the same line as the IP, IP-RANGE, and IP-MASK. After fixing the issues, both types of line feeds and comments are now supported.
66953	The maximum number of tags that PAN-OS and Panorama support for each virtual system and device group (including the Shared group) is now 2,500 instead of 1,000.
66924	When logging in to the Panorama web interface with two-factor RADIUS authentication, Panorama would successfully authenticate the user but then immediately log the user out of the web interface. With this fix, Panorama no longer logs the user out of the web interface following a successful authentication.
66918	Memory corruption issues related to SSL decryption caused the data plane to restart and resulted in a flapping condition between firewalls in an HA cluster.
66862	If the certificate name length had more than 31 characters and it was used in a decryption policy for SSL inbound inspection, a commit would fail. With this fix, validation fails when the certificate used in an SSL inbound inspection decryption policy has more than 31 characters inside the certificate name field.
66826	Due to SSL errors caused by the way the serial number is generated in the device certificate, you could not manage multiple WF-500 WildFire™ appliances from the same browser.
66761	To accommodate large quantities of scheduled reports with long reporting periods, the M-100 appliance now supports increased storage capacity.
66711	The passive device in a HA cluster triggers DOS alerts about a session limit reached for a classified DOS profile. After the fix, the passive device no longer receives the DOS logs since it is not processing any traffic.
66701	You can now increase the capacity of the Address Resolution Protocol (ARP) table and the MAC address table on PA-3020 and PA-3050 devices using the `debug system arp-mac-capacity increased` command. On the PA-3020 platform, running this command increases the maximum number of table entries from 1500 to 3000. On the PA-3050 platform, running this command increases the maximum number of table entries from 2500 to 5000.
66693	When a Port Address Translation (PAT) rule was configured to only change the destination port but not IP address for that host, Address Resolution Protocol (ARP) was not learned from a destination host on a connected network. With this fix, ARP resolves correctly.
66635	Enabling SSL Forward Proxy decryption with a self-signed certificate could sometimes cause the certificate presented to the client to have a negative serial number.
66520	An update has been made so that when you commit with an IP address/Netmask configured but do not select an HA port in HA settings, PAN-OS shows additional details on the commit fail error message that indicate the specific incomplete HA settings.

Issue Identifier	Issue Description
66482	In some cases you could not access the web interface for an M-100 appliance even though you could access the appliance through the CLI. The issue is now addressed so that you can access both the web interface and the CLI on an M-100 appliance.
66372	Fixed an issue where some threat names did not display correctly in threat logs forwarded from the firewall when the logs were viewed on a syslog server.
66360	Fixed an issue on the Panorama web interface, where hovering the mouse over the **High Availability** widget on the Dashboard was displaying incorrect information for threat versions.
66358	When a copper small form-factor pluggable (SFP) link speed was forced to 1000 Mbits/s, the interface state remained up even if there was no network cable attached. With the fix, the interface state now reflects the actual state of the network connectivity.
66208	A brute-force attack on an unprotected management interface on the firewall caused the /var/log/btmp log file to inflate and consume available disk space. With this fix, PAN-OS enables a log rotation function for failed SSH logins, such as those from brute-force attacks.
66021	After a client certificate was revoked, the GlobalProtect™ portal allowed users to log in one more time. After resolving this issue, GlobalProtect blocks all login attempts after revoking the client certificate.
66005	Previously, `show_log_system.txt` in the techsupport file contained 50,000 lines showing the oldest events and did not display the latest events if `show log system` had more than 50,000 lines in the system. The logs now display the recent events first.
66002	An issue with the Host Information Profile (HIP) report caused firewalls running PAN-OS to retain host information even after a GlobalProtect user logged out. In this case, the same client IP address was assigned to another user due to the HIP match and the traffic was handled according to the security policy that applied to the previous user.
65922	Improvements have been made to session management for PA-5000 platform devices.
65909	When configuring an HIP profile to check two drives for disk encryption, evaluation fails although the HIP report is correct. After the fix, the evaluation succeeds when configuring the HIP profile to check for two drives.
65866	Using the web interface, you can now configure the option to discard embedded ICMP error packets in the zone protection profile. Previously, you could only configure this option using the CLI.
65721	When pushing Wi-Fi settings to Android mobile devices, GlobalProtect did not set security parameters when an SSID was hidden, and prompted users to authenticate when the SSID was visible. With this fix, GlobalProtect correctly pushes the Wi-Fi settings to Android mobile devices.
65302	On the Panorama web interface, filtering security policies to display the policies for a specific device group displayed shared policies that were not targeted to any device in that device group. With this fix, the Panorama web interface only shows shared policies that are targeted to a device in the selected device group.

Issue Identifier	Issue Description
65294	In syslog and devsrv.log output, a message about the last known update from the PAN-DB cloud was labeled as seconds instead of minutes. The description of the log pattern now displays the correct label.
65220	With SSH proxy enabled, traffic to some SSH servers failed. With this fix, traffic to the SSH servers no longer fails when SSH proxy is enabled.
65174	Resolved an issue where an `Invalid IP Address` error was shown when creating a redistribution profile from within the Export Rules in OSPF or Redistribution Rules in BGP.
65031	During a high availability (HA) active/passive failover, a timing issue delayed the reestablishment of end-to-end connectivity for OSPF interfaces. The graceful restart hello delay timer now allows you to configure the length of time during which the firewall sends grace LSA packets. From the CLI, use the `gr-delay` option to specify the graceful restart delay on OSPF interfaces.
64759	Fixed an issue where a high availability (HA) failover occurred due to insufficient kernel memory on a PA-5000 Series firewall that was attempting to handle unusually heavy network and system traffic. With this fix, the kernel memory on PA-5000 Series firewalls is increased to ensure sufficient kernel memory is avail-able for ping requests and keep-alive messages even when under an unusually heavy load.
64751	Addressed an issue where SNMPv3 traps sent from the firewall for the EngineBoots and EngineTime variables were incorrectly set in the SNMP header.
64713	Removed the RC4-MD5 cipher from management and GlobalProtect SSL interfaces.
64606	When navigating to the GlobalProtect portal using a browser that had Transport Layer Security (TLS) 1.2 enabled, and when using a client certificate for authentication, the SSL connection failed due to issues with the fallback to a lower TLS version. With this fix, the fallback succeeds with Google Chrome and Mozilla Firefox. This specific behavior of Internet Explorer still exhibits issues.
64600	When a dynamic block list was configured on the firewall to be updated according to a list on a configured proxy server, the firewall was unable to access the proxy server. This issue has been resolved so that the firewall can correctly access the list on the proxy server to update the dynamic block list.
64439	When you configured QoS on an interface that was saturated with traffic from QoS classes without bandwidth guarantees, traffic from QoS classes with guaranteed bandwidth experienced traffic loss. This was due to rounding errors, which caused the total calculated interface bandwidth to exceed the actual bandwidth. With this fix, the bandwidth limits are properly calculated and no traffic loss is observed.
64389	In certain situations, when performing an HA failover, GlobalProtect clients connecting to the gateway using IPSec were disconnected and did not reconnect after the failover of the gateway. This issue has been fixed, and the GlobalProtect client reconnects to the new active gateway.

Issue Identifier	Issue Description
64310	When performing an application dump (to capture packets for a particular application) for a specific security rule, an application dump was performed for all security rules. This issue has been fixed so that specifying a security rule for an application dump only performs an application dump for traffic matching that rule.
64279	An enhancement has been made to lower the configurable amount of time at which the firewall refreshes FQDN object entries. The previous lowest amount of time you could configure for FQDN refreshes to occur was every 1800 seconds. You can now use the fqdn-refresh-time command to configure FQDN refreshes to occur every 600 seconds – 14,399 seconds.
64229	A QoS policy was not being enforced on the firewall and all traffic was being classified and treated as class 4 traffic (the default QoS class). This issue has been resolved so that a configured QoS policy is correctly enforced on traffic.
64223	Fixed an issue where FQDN objects that were added to a dynamic address group were not listed after issuing the command `request system fqdn show`, with the command displaying a message that no FQDN object is used in the policies.
64040	Addressed an issue where a log collector's disk usage exceeded the total log storage quota configured on Panorama (**Templates > Panorama > Collector Groups > Log Storage Settings**).
63857	In certain circumstances, an application could have been implicitly allowed through the firewall due to a configured rule that allowed only a dependent application. The issue has been fixed so that an application that might be implicitly allowed is properly blocked if needed.
63790	A firewall that did not have a GlobalProtect license and was configured with one portal and one gateway was displaying a commit warning when the cutoff time for a GlobalProtect gateway was set to any other value than the default value of 5 seconds (the cutoff time is how long a GlobalProtect agent will wait for the GlobalProtect gateways to respond in determining the best gateway to connect to). This issue has been fixed so that a commit warning is not displayed when the cutoff time for a GlobalProtect gateway is set to a value other than the default.
63641	When an LDAP authentication profile was configured with the **Password Expiry Warning** set to the default of 7 days, a warning message was not shown 7 days before the password was set to expire. This issue has been fixed so that users are correctly warned before their passwords expire, depending on the number of days entered in the **Password Expiry Warning** field.
63349	Fixed an issue where Dynamic Host Configuration Protocol (DHCP) leases were being reset when the firewall was restarted.
63218	The web interface allowed for a security policy to be created with the **Service** defined both as application-default and a specific service. This has been fixed so that you can either select the application-default option so that selected applications are either allowed or denied on their default ports or select a specific service or service group to limit to specific TCP/UDP port numbers (you cannot enable both of these options within a single security policy).

Issue Identifier	Issue Description
63123	The CLI command `test security-policy-match` with the `show-all` flag does not list all policies that match the defined criteria. The algorithm starts at the top of the rulebase and checks all rules until it finds the first rule that matches the defined criteria. The algorithm does not continue to check subsequent rules after this match occurs. Because this command only displays a list of potential matches and is not an exhaustive list, the explanatory text has been updated to reflect this behavior.
63010	An issue was seen while uploading large files to the WildFire cloud, where the firewall received an error that the file size exceeded the limit. As a result, the cloud connection continued to reset, blocking all other files in the upload queue. With this fix, files that exceed the limit to upload to the cloud are dropped and next file continues to be processed.
62791	An update was made to reduce the number of TCP stale sessions for PA-5000 series devices.
62644	When a copper SFP port was plugged in, the SFP interface's link displayed `unknown/unknown/up`; this has been updated to more accurately display `auto/auto/up`.
62222	Fixed an issue where a malicious DNS lookup did not generate a threat log when an anti-spyware profile was defined to allow low severity spyware.
62146	An update was made so that the firewall sends the NetFlow/IPFIX private enterprise number field value as a 32-bit number. It was previously sending the private enterprise number field value as a 16-bit number.
62018	The RADIUS Server Profile dialog indicated an error if you entered more than 15 characters for the Secret value, even though the character limit is 64. The dialog no longer displays an error as long as you enter no more than 64 characters.
61631	Fixed an issue that occurred when HA control packets were routed through the dataplane, causing OSPF neighbors to continually flap.
61489	Attempting to generate an certificate on Panorama using the CLI displayed the following error: `Internal error. Failed to insert xml node`. You can now generate certificates correctly for Panorama using the CLI.
61328	The restart speed has been optimized for Panorama when using NFS logs storage. This includes removing an unnecessary scanning of the threat log directory that was leading to a long start-up process.
61186	When managing multiple log collectors with Panorama, changing the name of a log collector group or deleting a log collector group caused a loss of logs. To prevent this, you can no longer change the name of an existing log collector group. Additionally, a warning is now displayed when attempting to delete a log collector group.
60893	A Java applet was incorrectly classified as malware by WildFire. This was due to an issue where the applet attempted to read a username, which requires permission from the Java virtual machine. The specific Java applet that was incorrectly classified has been reviewed and identified as a benign file.
60710	The CLI command `request certificate generate` failed to generate a certificate on Panorama. The command now generates a certificate as expected.

Issue Identifier	Issue Description
60341	Fixed an issue where renewing a server certificate was only effective for GlobalProtect portals and gateways by restarting the firewall. This issue has been fixed so that renewing server certificates for GlobalProtect portals and gateways works correctly without restarting the firewall.
60042	Fixed an issue where applying filters to search for or view security policies was not correctly displaying all the policies that matched the filter.
60022	Resolved an issue where for Session Initiation Protocol (SIP) traffic from a mobile device, a policy-based forwarding rule was only being applied to the client to server traffic flow, and not to the server to client traffic flow for the same session.
59304	Fixed an issue where User-ID lost group mapping information following an OpenLDAP refresh. This was due to the OpenLDAP server allowing the same name to be used as an object name and a user account and has been resolved.
58547	Policy-based forwarding (PBF) with symmetric return did not work when the traffic was translated with source NAT. Return traffic, which needs to be forwarded via the same interface on which it arrived, was dropped with the message `Symmetric Return: Packet dropped, no return MAC found`. The issue is fixed.
57917	Some tables in a firewall PDF summary report did not display correctly. Fixed an issue where no line was displayed between two points in a line graph, and another issue where the Top 5 Applications table was not correctly sorted to display the applications in descending order.
55370	With SSH proxy configured, if the SSH client performed a key renegotiation, the client would be disconnected and an error would be displayed that the server's host key did not match the signature supplied. An update was made to allow the new key to be accepted.
55249	You can now run the CLI command `test <feature>` for the following features: `botnet, cp-policy-match, custom-url, data-filtering, decryption-policy-match, dns-proxy, dos-policy-match, global-protect-mdm, global-protect-satellite, nat-policy-match, nd, pbf-policy-match, pppoe, qos-policy-match, routing, scp-server-connection, security-policy-match, stats-service, tag-filter, url, url-info-cloud, url-info-host, user-id, vpn, wildfire`.
54483	Resolved an issue where a fragmented DHCP response could cause packet processing services on the dataplane to restart.
33211	If the running configuration had more than 16,777,215 lines, the CLI command `show config running` failed to display the configuration: it displayed an out of range error. This has been fixed so that `show config running` displays the configuration regardless of size.

Getting Help

The following topics provide information on where to find out more about our products and how to request support:

Related Documentation

Refer to the following documents on the Technical Documentation portal at https://www.paloaltonetworks.com/documentation for more information on our products:

- New Features Guide—Detailed information on configuring the features introduced in this release.
- PAN-OS Administrator's Guide—Provides the concepts and solutions to get the most out of your Palo Alto Networks next-generation firewalls. This includes taking you through the initial configuration and basic set up on your Palo Alto Networks firewalls.
- Panorama Administrator's Guide—Provides the basic framework to quickly set up the Panorama virtual appliance or the M-100 appliance for centralized administration of the Palo Alto Networks firewalls.
- WildFire Administrator's Guide—Provides information on deploying, operating, and maintaining the WildFire cloud and the WildFire WF-500 appliance and the Palo Alto Networks firewalls.
- VM-Series Deployment Guide—Provides details on deploying and licensing the VM-Series firewall on all supported hypervisors. It includes example of supported topologies on each hypervisor.
- GlobalProtect Administrator's Guide—Takes you through the configuration and maintenance of your GlobalProtect infrastructure.
- Online Help System—Detailed, context-sensitive help system integrated with the firewall web interface.
- Open Source Software (OSS) Listings—OSS licenses used with Palo Alto Networks products and software:
  - PAN-OS 6.1
  - Panorama 6.1
  - WildFire 6.1

Requesting Support

For technical support, call 1-866-898-9087 or send email to support@paloaltonetworks.com.

Contact Information

Corporate Headquarters:

Palo Alto Networks
4401 Great America Parkway
Santa Clara, CA 95054

http://www.paloaltonetworks.com/contact/contact/

Palo Alto Networks, Inc.
www.paloaltonetworks.com

Revision Date: May 13, 2015